SSC PACIFIC SECURITY SUPPORT
Statement of Work (SOW)

1.0 INTRODUCTION

The Department of the Navy, Space and Naval Warfare (SPAWAR) System Center Pacific (SSC Pacific) is acquiring security support services for Code 833, Security Programs, and Code 87, Special Programs, Oversight, and Compliance Competencies.

1.1 *Scope*. This effort provides on-site support of SSC Pacific's Security Programs. The effort includes support for the Security Control System, Lock and Key Control, Foreign Travel, Personnel Security, Information Security, Communication Security, Physical Security, Foreign Visit Coordination, Continuity of Operations Planning (COOP), Scientific and Technical Intelligence Liaison Officer (STILO), Special Security Office (SSO), Operations Security (OPSEC), Research and Technology Protection (RTP) and Supply Chain Risk Management (SCRM) to SSC Pacific, SPAWAR Headquarters (HQ), and supported Program Executive Offices (PEOs).

1.2 *Background*. SSC Pacific is a shore-based activity whose mission is to be the Nation's pre-eminent provider of integrated C4ISR solutions for the fleet. The Security Control System Program is responsible for controlling identification related to access to the facility. This office issues identification badges and is the primary control point for all visitors, SSC Pacific employees, and tenant command personnel. The Lock and Key Control Program maintains Locksmith Services database and interacts with SSC Pacific personnel in the issuance of locks, keys, safes and safe combinations. The Personnel Security Program is responsible for the in-processing and out-processing of Government security clearance applications. The Foreign Travel Program is responsible for generation of foreign travel/area clearance messages, using the Non-Secure Internet Protocol Router (NIPR) and Secure Internet Protocol Router Network (SIPRNET) computers to research material for briefing individuals, assisting in preparation of Personal Protection Plan, providing classified site-specific foreign travel briefings, and maintaining a database for tracking travel to foreign countries. The Information Security Program is responsible for executing the Information Security program through documentation review, classified shipment reviews, site assist visits and inspections, issuance of courier cards and letters, development of necessary training materials, and maintenance of various databases. OPSEC, RTP, STILO, and SSO requirements must be addressed for various Research, Development, Test and Evaluation (RDT&E), and acquisition efforts. Oversight and subject matter expertise support is necessary in order for the supported commands and their personnel to meet these requirements, and to integrate the supporting processes into all operations and activities at SSC Pacific, SPAWAR, and supported PEOs. OPSEC and RTP focuses on the production, handling or processes for critical information/technologies, Critical Program Information (CPI), and SCRM requirements to ensure the protection of sensitive unclassified information and also technologies that enable or support warfighting capabilities. The STILO program was established in the early 1970s to strengthen the interface and flow of intelligence between the Intelligence Community (IC) and the Naval Materiel (NAVMAT) Command activities, and supports the same for DON RDT&E and acquisition efforts. The SSO was established by national directive to perform the security functions related to the protection of Sensitive Compartment Information (SCI) and the oversight of the Sensitive Compartment Information Facilities (SCIFs).

2.0 APPLICABLE DIRECTIVES

The Contractor shall adhere to all policies, procedures and regulations in force at the time of the contract across the SPAWAR Claimancy. The Contractor shall also adhere to the following documents, current and future updates:

Document Type	No./Version	Title	SOW Para.
DoDI	2000.16	Pre-Departure Briefing Requirements	3.4
DoDI	4500.54-G	Foreign Clearance Guide	3.9
Agency Order		SPAWARSYSCEN Pacific Training Guide for the Security Control System	3.2
Agency Order		SPAWARSYSCEN Pacific Lock and Key Control desk guides	3.3
NSPD/HSPD	NSPD-51 / HSPD-2	National Security Presidential Directive-51/Homeland Security Presidential Directive-20	3.5
DOD	5200.2-R	Personnel Security Program	3.5, 3.12
SECNAVINST	5510.30B	Department of the Navy (DON) Personnel Security Program (PSP) Instruction	3.5, 3.12
DODM	5200.01 Volume 1	DoD Information Security Program: Overview, Classification, and Declassification	3.6, 3.12
DODM	5200.01 Volume 3	DoD Information Security Program: Protection of Classified Information	3.6, 3.12
DODM	5200.01 Volume 4	DoD Information Security Program: Controlled Unclassified Information (CUI)	3.6, 3.12
SECNAVINST	5510.36A	Department of the Navy (Don) Information Security Program (ISP) Instruction	3.6, 3.12
DODD	8500.1	Information Assurance (IA)	4.0, 3.12
SECNAVINST	5239.3B	Department of the Navy Information Assurance Policy	4.0, 3.12
COMFLTFORCOM	091608z OCT 03	Personal Protection Plan Requirements	3.4
NIST	SP 800-53 Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations	3.14
SECNAVINST	M-5510.30	Personnel Security Program	3.5, 3.12
SECNAVINST	M-5510.36	Information Security Program	3.6, 3.12
DOD	5220.22-M	National Industrial Security Program Operating Manual	3.12, 7.0
DODI	5200.02	DoD Personnel Security Program (PSP)	3.5, 3.12
OPNAVINST	5239.1C	Navy Information Assurance (IA) Program	4.0, 3.12
DODI	5000.02	Operation of the Defense Acquisition System	3.11, 3.14
SECNAVINST	5000.2E	Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System	3.11, 3.14

OPNAVINST	3880.6A	STILO Program and Intel Support for the Naval Research, Development, Test & Evaluation and Acquisition Communities	3.11
OPNAVINST	3811.1E	Threat Support to the Defense Acquisition System	3.11
SPAWARINST	3800.1D	Intelligence Support to SPAWAR Programs	3.11, 3.12, 3.13, 3.14
DODI	5105.21 Volumes 1-3	Sensitive Compartmented Information Administrative Security Manual	3.12
ICD	503	Protecting Sensitive Compartmented Information within Information Systems	3.12
ICD	701	Security Policy Directive for Unauthorized Disclosure of Classified Information	3.6, 3.12
ICD	704	Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)	3.12
ICD	705	Physical Security Standards for Sensitive Compartmented Information Facilities	3.12
SPAWARINST	3432.1A	Operations Security	3.13
SECNAVINST	3070.2	Operations Security Policy	3.13
OPNAVINST	3432.1A	Operations Security Instruction	3.13
DoD 5205.02-M	5205.02-M	Operations Security Program Manual	3.13
National Security Decision Directive (NSDD) 298	NSDD 298	National OPSEC Program	3.13
DODI	5200.44	Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)	3.14
DODI	5200.39	Critical Program Information (CPI) Protection Within the Department of Defense	3.14
DON	CPI Assessment SOP	Standard Operating Procedures (SOP) for the Standardized Critical Program Information Identification Process in Department of Navy Acquisition Programs	3.14
DODI	6205.4	Department of Defense Instruction, Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense	4.0
DON	CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT)	4.0
SPAWARINST	4440.12	Management of Operating Materials and Supplies (OM&S), Government Furnished Property (GFP), Contractor	4.0

		Acquired Property (CAP), Property, Plant and Equipment (PP&E), and Inventory	
Navy Telecommunications Directive	(NTD) 10-11	System Authorization Access Request (SAAR) - Navy	4.0
DON	CA Process	DASN RDT&E Technology and Program Protection Program Protection Plan (PPP) Criticality Analysis (CA) Overview and Tutorial	3.14

3.0 TECHNICAL REQUIREMENTS

The contractor shall provide technical support relevant to the Security Control System, Lock and Key Control, Foreign Travel, Personnel Security, Information Security, Electronic Key Management System (EKMS), Physical Security, Foreign Visit Coordination and Disclosure, Continuity of Operations Planning (COOP), Scientific and Technical Intelligence Liaison Officer (STILO), Special Security Office (SSO), Operations Security (OPSEC), Research and Technology Protection (RTP), and Supply Chain Risk Management (SCRM), to SSC Pacific, SPAWAR HQ, and its supported Program Executive Offices (PEOs).

3.1 GENERAL

The contractor shall prepare and deliver the Contractor's Monthly Status Report, which indicates the cost, schedule, performance, personnel, travel and other direct cost status. (CDRL A001)

The contractor shall deliver all contract and technical information in digital form. All applications must be compatible with the latest Navy Marine Corps Intranet (NMCI) approved revisions or as coordinated with the Government. All required data and documentation will be delivered via email, CD or DVD. All data shall be in Microsoft Word, Microsoft Excel or Microsoft PowerPoint. At the Government's discretion, Adobe PDF may be utilized for some materials. Any electronic submittals, including attachments, submitted via e-mail shall be readable on a standard personal computer using Windows 7; OSX or later, Microsoft Office Suite 2007 or later, Microsoft Project 2007 or later. All contractor personnel shall be proficient in the use of Microsoft Windows environment and all Microsoft Office applications.

3.2 SECURITY CONTROL SYSTEM PROGRAM

The Security Control System records, tracks and generates the documentation required to issue badges to access the Naval Base Point Loma (NBPL). The contractor shall generate and issue SSC Pacific identification badges and Common Access Cards (CAC) ranging from 130 – 150 transactions per day and process up to 150 visit requests actions per day. The contractor shall provide professional customer support while interacting with all levels of civilian and military personnel via phone, email and in person and provide assistance to visitors to include marking building locations on maps, and providing general information regarding visit procedures. Work performed in this section requires a SECRET clearance.

3.2.1 *Visitor Requests.* The contractor shall receive and process all visit requests received through the DoD Joint Clearance and Access Verification System

(JCAVS) database or by facsimile. Processing includes submitting the requests to NBPL for vetting through the Consolidated Law Enforcement Operations Center Database (CLEOC), National Sex Offender Public Website (NSOPW) and the NBPL Disqualification listing. Once the request is vetted, the contractor shall issue a SSC Pacific badge or CAC.

3.2.2 *SSC Pacific Badges.* The contractor shall create and issue SSC Pacific badges to properly vetted personnel and magnetically encode them through a magnetic strip encoder. This function includes inputting personal data such as, company and contract information into a Government-developed security database. Each visitor request action requires multiple files to be updated in a structured format in accordance with government written procedures.

3.2.3 *Common Access Cards.* The contractor shall issue CACs to properly vetted personnel. This function includes inputting personnel data into the Defense Enrollment Eligibility Reporting System (DEERS) database, verifying the data and issuing the Department of the Defense (DoD), Chief Information Office (CIO) CACs. If problems arise with the hardware and/or software, the contractor shall contact the CAC Program Office to resolve the issue.

3.3 LOCK AND KEY CONTROL PROGRAM

The objective of this effort is to track service requests, maintain lock, key and safe inventory, issue keys, record and issue requests to move security containers, and issue work orders to the locksmith personnel. The contractor shall provide professional customer support while interacting with all levels of civilian and military personnel via phone, email and in person. Work performed under this section requires a TOP SECRET clearance.

3.3.1 *Lock and key coordination.* The contractor shall issue and retrieve keys from personnel and maintain the database of any changes. The contractor shall receive and enter data from the locksmith service request forms into a Government-developed Microsoft access database. This effort involves processing approximately 200 requests per month. The contractor shall verify, research, and analyze the data as necessary to ensure that the information is accurate. The contractor shall coordinate with the Government for any clarification needed with these requests.

3.3.2 *Data management.* The contractor shall maintain the locksmith services database, which consists of approximately 10,000 records pertaining to strong rooms, security containers, locks, and keys. The contractor shall generate reports and provide to the Government as required. The contractor shall maintain the database inventory to include moving, issuing, and the turning-in of security containers, issuing combinations, and keys. Combinations to security containers shall be stored and controlled by the contractor in the database.

3.3.3 *Security Containers.* The contractor shall act as the point of contact for the procedures in accessing or declassifying containers and will also serve as the lock/key/combo point of contact for employee checkout. The contractor shall receive, enter, and forward requests for the movement of security containers to the appropriate Facilities Manager and the locksmith.

3.4 FOREIGN TRAVEL PROGRAM

The contractor shall manage the foreign travel program. This program includes the processing of approximately 600 requests per month for over 130 countries in accordance with each country's specific timelines and criteria. This program includes receiving foreign travel requests, verifying all personal and security information, and electronically creating and sending messages using Aircraft and Personnel Automated Clearance System (APACS) and the Electronic Country Clearance (ECC) system. Work performed under this section requires a SECRET clearance and access to NIPR/SIPRNET.

3.4.1 *Request for Foreign Travel (RFT).* The contractor shall process RFT forms. This includes entering the information into the Government database, typing memos and preparing and maintaining individual files. Maintain the logs of all prepared messages and maintain a database spreadsheet of all foreign travel information, to include receiving travelers' arrival, movement and completion dates. The contractor shall validate information provided on the request forms by using existing database application.

3.4.2 *Training.* The contractor shall verify the travelers training record for completion of foreign travel briefing and training needs and notify travelers of training outstanding requirements. Additionally, the contractor shall research travel briefing requirements and create classified site-specific foreign travel briefings using country-specific data information and provide assistance to the traveler with preparation of their Personal Protection Plan.

3.5 PERSONNEL SECURITY PROGRAM

The objective of this program is to support and assist the government employee in initiation and processing of government security clearance applications and maintain necessary files and documentation within the Personnel Security Office. Work performed under this section requires a TOP SECRET clearance.

The contractor shall maintain files and documentation within the Personnel Security Office and provide support for the in-processing and out-processing of personnel. This includes support for the processing of new personnel security clearances as well as periodic reinvestigations, and implementing the continuous evaluation program and reporting of derogatory/adverse information to the government technical point of contact for further submission to DoD Consolidated Adjudication Facility (CAF). The contractor shall provide customer service to SSC Pacific employees in support of all personnel security clearance services and assist with courier cards and letters as required.

3.6 INFORMATION SECURITY PROGRAM

The contractor shall execute the Department of Defense (DoD) and Navy Information Security program through documentation review, site assist visits and inspections, classified shipping reviews, issuance of courier cards and letters, development of necessary training materials, and maintenance of various databases.

The objective of this program is to support and assist the Government with classified and Controlled Unclassified Information (CUI) during initial classification and controlling, as well as subsequent review of material to support decontrolling, downgrading and declassification of documentation and media. The contractor shall maintain knowledge of the DoD/Navy Information Security program and provide command services consistent with governing directives. Work performed under this section requires a TOP SECRET clearance.

3.6.1 *Document control.* The contractor shall coordinate with various program managers, project leads, branch heads, subject matter experts and the Public Affairs Office in support of CUI document/media reviews against the official National Archives and Records Administration's CUI registry and applicable service/agency guidelines to support appropriate markings during controlling, decontrolling, safeguarding and publication to include release of controlled technical information. The contractor shall support the Government in making tentative and final classification, patent secrecy determinations, and resolving conflicts between Original Classification Authorities (OCA). This includes consulting with applicable OCA, as applicable, to support appropriate markings during the classification, downgrading, declassification and publication. The contractor shall conduct the research utilizing the NIPR/SIPRNET.

3.6.2 *Site assist visits and inspections.* The contractor shall prepare and perform site assist visits and inspections of collateral open storage (secure rooms) to ensure compliance with governing requirements for proper handling, safeguarding, transportation and destruction of classified national security information and CUI.

3.6.3 *Classified shipping.* The contractor shall ensure compliance with established local practices for shipment of classified material as listed in the SSC Pacific Security Manual.

3.6.4 *Courier cards and letters.* The contractor shall receive, process and record requests for courier cards, orders and airline letters and maintain the appropriate database.

3.6.5 *Review and Training support.* The contractor shall conduct reviews of the command CUI program, assist the Government in the development of associated briefs, prepare and update necessary training materials and maintain databases. The contractor shall maintain the command library of applicable Security Classification Guides for all projects/programs and assist with the creation of security plans in support of classified meetings and conferences held at SSC Pacific.

3.7 COMMUNICATION SECURITY (COMSEC)

Communication security provides for the EKMS vault and administrative assistance support to the communications security material systems custodian in accordance with EKMS 1 series guidance. Work performed under this section requires a TOP SECRET clearance with Sensitive Compartmented Information (SCI) access.

3.7.1 Technical and Administrative EKMS Support. Maintain a valid courier card and operate government vehicles to transport COMSEC material to and from the SSC Pacific COMSEC account. Assist the Key Management Infrastructure (KMI) Manager with the receipting for and transferring of COMSEC material in/out of the account as well as to/from the local elements, utilizing the KMI system and standard accounting forms. Perform routine backups of the KMI system and upgrades to fill devices, secure voice equipment, and in-line encryption (INE) devices. Assist the KMI Manager in the creation and distribution of black keys for Local Elements (LE) use. Sign receipts, inventories, and destruction reports for COMSEC material as a witness only. Maintain Two Person Integrity requirements for top secret keying material as required. Assist the KMI Manager in the performance and execution of the command semiannual inventories to include: conducting page checks, coordinating LE inventories with custodians, sighting material issued, and correcting discrepancies.

3.8 PHYSICAL SECURITY

The objective of this program is to provide resource protection as well as to perform documenting / managing / scheduling / record keeping secure room inspections and discrepancies. Assist the Anti-terrorism and Force Protection Officer with planning and conducting exercises within SSC Pacific such as Active Shooter, Bomb Threat, or other simulated or actual emergencies. Work performed in this section requires a SECRET clearance.

The contractor shall assist in documenting, managing, and scheduling of the secure room inspections and discrepancies, record daily activity incidents, and debarment letters of SSC Pacific personnel. The contractor shall assist with conducting physical security inspections of occupied buildings at SSC Pacific and maintaining the instruction library on all areas relating to Physical Security, Law Enforcement, and Antiterrorism.

3.8.1 The contractor shall coordinate the local security objectives and plans in order to develop and implement policies, procedures, systems and programs, maintain awareness in security program interrelationships, requirements, regulations and guidance to apply in the protection of facilities and materials from espionage, sabotage and destruction, conduct physical security surveys, inspections and assessments to evaluate the effectiveness of existing classified material control practices, and prepare narrative reports (i.e. identifying security deficiencies) of findings and recommendations for corrections of the deficiencies.

3.9 FOREIGN VISITS COORDINATION

The objective of this effort is to ensure appropriate access to the facility and ensure that the disclosure of unclassified and classified information is granted to those foreign nationals that meet certain criteria, stipulation and are in compliance with DoN Policies and Directives. The contractor shall perform daily reviews and updates, using the Security Policy Automation Network (SPAN) database, to ensure visits are received and processed in a timely and efficient manner. Work performed in this section requires a TOP SECRET clearance and access to NIPR/SIPRNET.

The contractor shall receive and disseminate all SSC Pacific foreign visits through the Foreign Visits System (FVS). Coordinate with visit sponsor and prepare package for submission to the SPAWAR HQ Designated Disclosure Authority review. The contractor shall obtain and confirm for foreign visits and foreign disclosure requests. Enter all foreign visitor data in the Security Control System for issuance of foreign visitor badge. Each visitor request action requires multiple files to be updated such as visit request ID case number, country, nationality and other personal information taken from the passport that required for issuance of badge. Complete foreign visit weekly status reports. The contractor shall coordinate with SPAWAR HQ Foreign

Disclosure Officer to obtain a copy of the Delegation of Disclosure Authority Letter (DDL) to ensure foreign officials and foreign military officers are only granted access to authorized areas, material and information.

3.10 CONTINUITY OF OPERATIONS (COOP)

The contractor shall develop, maintain and execute all planning requirements on the integration of continuity of operations in the research, development, acquisition, and logistical support of equipment, systems, and facilities. The contractor shall provide all Management, Supervision, and Labor necessary to support continuity of operations and functions in any emergency event affecting San Diego, develop a plan and provide guidance on integration of continuity requirements in the research, acquisition and logistical support of equipment, systems and facilities, act as the focal point for providing Base Operating Support across competencies and business units, implement necessary steps to move to an interim or alternative operating facility (AOF) and to reconstitute the organization. Work performed in this section requires a SECRET clearance.

3.11 SCIENTIFIC AND TECHNICAL INTELLIGENCE LIAISON OFFICER (STILO)

The STILO office supports development and acquisition in the areas of C4ISR and critical national security systems by facilitating the acquisition of intelligence related threat data and interpretation of intelligence information for acquisition program managers and scientific, technical and engineering personnel. STILO support encompasses technological and programmatic information, and the use and protection of intelligence related threat data consistent with prevailing Department of Defense (DoD) and Department of Navy (DoN) policies and procedures. Work performed in this section requires a TOP SECRET clearance with SCI access.

STILO support shall include collaborating with scientific, technical and engineering personnel and will encompass a range of services including research via the Joint Worldwide Intelligence Communications Systems (JWICS) and SIPRNET, researching and disseminating validated Cyber Intelligence products, and regular reviews of key Intelligence Community (IC) classified web sites. The contractor shall provide customers with recommendations of new sources for intelligence which should be used by their programs and projects.

3.11.1 *Cyber Intelligence.* The contractor shall proactively, and in response to Requests for Intelligence (RFI), research and disseminate validated Cyber Intelligence products to command customers, regularly review key IC classified web sites in order to provide new Threats to leadership/projects/programs and develop tailored briefings to be presented to command personnel based on Cyber Intelligence research.

3.11.2 The contractor shall accurately interpret technical language of Cyber (Electronic Warfare and Computer Network Operations), C4ISR, and National Intelligence Community to identify customer requirements and accurately match these with relevant Intelligence products.

3.12 SPECIAL SECURITY OFFICE (SSO)

SSO support encompasses a range of services including classified documentation tracking and maintenance, personnel security questionnaire preparation to include conducting prescreening interviews, visit request preparation and control, preparation of courier letters, classified meeting coordination, processing of foreign travel and foreign contact information, courier runs, packaging Sensitive Compartmented Information (SCI) material for shipment, operating classified hardware (e.g. secure teleconference hardware and access control devices), Sensitive Compartmented Information Facilities (SCIF) access control, and reviewing, updating, and implementing SSO regulations, to include those related to SSO processes and training and awareness, and working directly with the SPAWAR/SSC Pacific SSO for tasking and approval of completed work efforts and collaboration with process improvement. Work performed in this section requires a TOP SECRET clearance with SCI access.

3.12.1 *SCI Support.* The contractor shall accurately pass and receive SCI visit clearances, to include updating the SSO database with clearance information, assist in the preparation for SCI indoctrinations and debriefs, assist in the preparation of materials for periodic or annual security briefings related to SCI requirements, and assist in the accurate control and accountability of SCI documentation, properly destroy SCI material or documentation. Additionally, the contractor shall process personnel security background investigative paperwork, which includes fingerprinting and conducting security prescreening interviews, and forwarding completed SF86 packages to the appropriate processing activity. Contractor shall access and utilize the Joint Personnel Adjudication System (JPAS).

3.12.2 *Classified Facilities.* The contractor shall support several GENSER security spaces and SCIFs to include courier runs, implementing physical security requirements and coordination of large symposium/meetings held within GENSER security spaces or SCIFs.

3.12.3 *Travel Compliance.* The contractor shall process all foreign travel and foreign contact forms received by the SSO from Government and contractor personnel with SCI access. The contractor shall review, enter into the SSO database and route all foreign travel and foreign contact forms, and identify and resolve issues as directed or required. SSO support covers special security services in the areas of administrative, information and physical security for and related to SCI.

3.13 OPERATIONS SECURITY (OPSEC)

OPSEC support encompasses a range of activities that are used by the Department of Defense (DoD) and implemented across SSC Pacific, SPAWAR HQ, and its supported PEOs, as a means to identify, control, and protect unclassified sensitive and Controlled Unclassified Information (CUI) associated with U.S. national security related programs and activities. OPSEC support includes both subject matter expertise and oversight to implement and integrate the OPSEC Program across all activities supported under this SOW. OPSEC is a five step analytical process consisting of identification of critical information; analyzing the threat; analyzing the vulnerabilities; assessing risks; and developing and implementing countermeasures. Work performed in this section requires a SECRET clearance.

3.13.1 *Pre-Publication review*. The contractor shall assist the OPSEC Office in the review of material (briefings, technical papers, articles, etc.) to ensure that OPSEC requirements are being met and that Critical information is not being released to the public. Reviews shall include research on the internet to determine if other or related materials on the same or related technologies have been released, analysis of multiple sources of data, and recommendations for potential changes in order for submitted material to be released to the public. Additionally, close coordination with the Command(s) Public Affairs Office(s) is required.

3.13.2 *Websites content review*. The contractor shall assist the OPSEC Office in conducting random and periodic reviews of any of the Command(s) websites and social media for Critical Information or OPSEC concerns. Additionally, research may be required as directed by the OPSEC Manager with regard to command personnel posts to the internet or social media.

3.13.3 *Education and awareness, process improvement.* The contractor shall assist the OPSEC Office with the development of OPSEC education and awareness products, to include briefings, posters, internet/social media posts or other materials. Development of products may include internet research regarding articles of use, interest for OPSEC purposes or integration into new OPSEC materials. Additionally, the contractor may be required to deliver OPSEC briefings and or place OPSEC materials at various command facilities and locations. The contractor shall provide recommendations for and assist with the development of command OPSEC process improvement efforts.

3.14 RESEARCH and TECHNOLOGY PROTECTION (RTP) and SUPPLY CHAIN RISK MANAGEMENT (SCRM)

RTP support includes subject matter expertise and oversight responsibilities across SSC Pacific, SPAWAR HQ, and its supported PEOs, implemented through collaboration with PORs and scientific, technical and engineering personnel to address RTP requirements. RTP requirements are addressed through direct contact with personnel both internal and external to the command(s) and working groups, and through assisting with the development of POR or Project Program Protection Plans (PPPs), developing SCRM protection methods, assisting with CPI assessments and Criticality Analysis (CA), and reporting directly to the SPAWAR RTP Lead for tasking and approval of completed work efforts and collaboration with process improvement. Work performed in this section requires a TOP SECRET clearance with SCI access.

3.14.1 *RTP Requirements*. The contractor shall provide recommendations and guidance on RTP requirements and systems engineering based analysis supporting technology protection measures, PPP development and SCRM methods to assist with the guidance, development of, and subject matter expertise in Program or Project PPPs and SCRM requirements, so they may be adequately addressed prior to program acquisition events or milestones.

3.14.2 *SCRM support*. The contractor shall advise SPAWAR Program Management Offices (PMOs) or Project managers in the performance of CAs including the analysis of the design, and if available, configuration of systems, based on the DoN CA in accordance with NIST SP 800-53 Rev. 4, section SA-14, and DoDI 5200.44. The contractor shall engage with SPAWAR PMOs, system managers or Project managers to assure that SCRM measures and mitigations are developed and documented in applicable Program or Project PPPs according to prevailing DoD and DoN SCRM guidance, and as necessary to address the SCRM-related controls contained in NIST SP 800-53 Rev. 4, section SA-12.

3.14.3 *Program or Project PPP support*. The contractor shall coordinate and assist with aspects of Program or Project PPP development, including CPI assessments, anti-tamper requirements, security classification guidance, threat assessments, and related areas. The contractor shall develop and deliver briefings to PMOs and Projects on RTP or RTP related requirements, including SCRM, Program or Project PPPs and related documents / templates and Standard Operating Procedures (SOPs).

3.14.4 *SCRM threat assessment support*. The contractor shall assist with the submission, management and tracking of SCRM threat assessment requests between a Program or Project, the SPAWAR RTP office, and the appropriate intelligence agency.

3.14.5 *Education and awareness, process improvement*. The contractor shall assist with development / implementation of RTP and SCRM initiatives, activities and processes across SSC Pacific, SPAWAR HQ, and its supported PEOs, and creating or updating associated process documentation, to include utilization of command internet assets (Webpage, Blog, Wiki, etc.). The contractor shall provide recommendations for and assist with the development of RTP process improvement efforts.

4.0 CYBER SECURITY

The contractor shall meet the Cyberspace Workforce (CSWF) standards in accordance with DoD 8570.01, DoD 8570.01-M, SECNAV M-5239.2 and SECNAVINST 5239.20. Contractors who perform information assurance duties or functions, whether primary or additional/embedded, on DoD computer systems (stand alone or networked) shall meet the certification requirements for each category/ level/ and operation environment as required. The contractor shall identify, document, submit, track, and report certification status and shall report change in contractor personnel or tasks that impacts CSWF to the Contracts Office Representative (COR).

DoDI Directive 8500.01, Subject: Cybersecurity, paragraph i states "Cybersecurity workforce functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened in accordance with DoD 5200.2-R for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information" in accordance with DoDM 5200.01 Vol. 1. DoD 5200.2-R and DoDD 5200.2 require all persons assigned to sensitive positions or assigned to sensitive duties be U.S. citizens. All persons access to controlled unclassified information (without regard to degree of IT access) or performing other duties that are considered "sensitive" as defined in DoDD 5200.2 and DoD 5200.2-R must be U.S. citizens. Furthermore, access by non-U.S. citizens to unclassified export controlled data will only be granted to persons pursuant to the export control laws of the U.S. The categories of controlled unclassified information are specified in DoDM 5200.01 Vol. 4. These same restrictions apply to "Representatives of a Foreign Interest" as defined by DoD 5220.22-M (National Industrial Security Program Operating Manual, NISPOM). DoD 8570.01-M further stipulates additional training and/or certification that is required by all persons assigned to Information Assurance functions.

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

IT Position Categories

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R, SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM shall assist the Government Project Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. Requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access are submitted by SPAWAR/SSC Atlantic/SSC Pacific Security Office, processed by the OPM, and adjudicated by DOD CAF. IT Position Categories are determined based on the following criteria:

IT-I Level (Privileged) - Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudication of Single Scope Background Investigation (SSBI) or SSBI-PR. The SSBI or SSBI-PR is updated a minimum of every 5 years. Assignment to designated IT-I positions requires U.S. citizenship unless a waiver request is approved by CNO.

IT-II Level (Limited Privileged) - Positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudication of a Position of Trust National Agency Check with Law and Credit (PT/NACLC). Assignment to designated IT-II positions requires U.S. citizenship unless a waiver request is approved by CNO.

IT-III Level (Non-privileged) - All other positions involved in computer activities. Incumbent in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudication of a Position of Trust National Agency Check with Written Inquiries (PT/NACI).

5.0 TRAVEL

This task may require contractor travel to locations within the continental United States. The contractor shall request travel in support of this task order. The request for all routine travel shall be made via email to the COR no later than five (5) working days in advance of the anticipated travel date for final approval. For emergent travel, requests shall be made within three (3) days of the actual travel date and will be approved by the COR. Trip/activity reports shall be completed and submitted to the COR five (5) days after completion of the trip. (CDRL A002)

The travel request shall include the following:

- Traveler's name
- Name of specific government technical POC requesting the travel
- Program/project name travel is required for
- Applicable SOW paragraph number
- Reason for travel
- Duration of travel
- Dates of travel
- Travel cost estimate
- Total travel funds expended to date
- Balance of authorized travel funding

6.0 GOVERNMENT FURNISHED INFORMATION/GOVERNMENT FURNISHED PROPERTY

GFI / GFP is not anticipated.

7.0 SECURITY

The nature of this task requires access to SSC Pacific databases, contract files that may include proprietary data, Privacy Act data, and unclassified information. Contractor is required to sign a non-disclosure agreement and comply with the requirements noted in the DD254. The work performed by the contractor will include access to unclassified and up to TOP SECRET/SCI data, information, meetings, and spaces. The contractor will be required to provide individuals with security clearances at the appropriate classification levels, as specified in the different security facets identified in the above paragraphs. Some contractors will be required to access communications security, SIPRNET and JWICS at government sites. Contractor may also come into contact with COMSEC, Restricted Data, CNWDI, Formerly Restricted Data, and SIPRNET. The contractor shall be North Atlantic Treaty Organization (NATO) briefed and complete the derivative classification training prior to being granted access to SIPRnet/JWICS; training is provided by the facility security officer.

Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current SSBI with ICD 704 eligibility (which replaced DCID 6/4 eligibility).

As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to Commanding Officer, Attn: Foreign Travel Team, Space and Naval Warfare Systems Center Pacific, 53560 Hull Street, Building 27, 2nd Floor -Room 206, San Diego, CA 92152 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten.mil (prefix): course number: US007; title: Level 1 Anti-terrorism Awareness Training, if experiencing problems accessing this website contact ssc_fortrav@navy.mil. Forward a copy of the training certificate to the previous email address or fax to (619) 553-6863. Sere 100.2 Level A code of conduct training is also required prior to Oconus travel for all personnel. Sere 100.2 Level A training can be accessed at http://jko.jfcom.mil (recommended), https://jkodirect.jten.mil/atlas2/faces/page/login/login.seam, recommend course: prefix: J3T: course #: A-US1329, for civilian, military, and contractors. Personnel utilizing this site must have a CAC. A Sere 100.2 Level A training disk can be borrowed at the SSC Pacific Point Loma Office or Old Town Campus Office. Specialized training for specific locations, such as SOUTHCOM human rights, or U.S. forces Korea entry training, may also be required; SSC Pacific security personnel will inform you if there are additional training requirements. Finally, EUCOM has mandated that all personnel going on official travel to the EUCOM AOR must now register with the Smart Traveler Enrollment Program (STEP). When you sign up, you will automatically receive the most current information the State Department compiles about your destination country. You will also receive updates, including Travel Warnings and Travel Alerts. Sign up is one-time only, after you have established your STEP account, you can easily add official or personal travel to anywhere in the world, not just EUCOM. http://travel.state.gov/content/passports/en/go/step.html.

7.1 *Operations Security (OPSEC) requirements*. OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process command(s) Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

8.0 PLACE OF PERFORMANCE

8.1 *Place of Performance*. The primary place of performance shall be at Government facilities in San Diego, CA, as designated by SSC Pacific.

8.2 *Workstations*. NMCI seats will be available for contractors working on site. The Government will provide desk space and administrative/office supplies to on-site contractor support personnel.

The Government will provide property, information, and/or material for the performance of this SOW including Navy/Marine Corps Intranet (NMCI) Common Access Cards (CACs), alternate tokens, and SIPRnet tokens as required. The Contractor PM/FSO is responsible for notifying the Government COR and the Trusted Agent (TA) when an employee who has been issued a CAC leaves the Company or transfers to another Program/Project. In the case of an employee who no longer works for the Company, the Company must collect the CAC and surrender it to the COR within two (2) working days of the employee's departure. In the case of an employee still retained by the company transferring to another Program/Project within SPAWAR, the company will notify the COR within two (2) working days so the TA can transfer the TA responsibilities to the new TA vice revoking and issuing a new CAC. Alternate tokens and SIPRNet tokens shall be surrendered upon departure to the Local Registration Authority (LRA) first, and if not available, to the COR.

9.0 OTHER

9.1 *Deliverables*. The Contractor shall provide the deliverables listed in the Contracts Data Requirements List (CDRL), Exhibit A Contracts Data Requirements List DD Form 1423. Deliverables shall be prepared in contractor format where not otherwise specified by the Government.

CDRL	Title	Due Date
A001	Contractor's Progress, Status, and Management Report	15 days after the end of month
A002	Trip Activity Report	5 days after travel is complete

9.2 *Enterprise-Wide Contract Management Application (ECMRA).* The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the SSC Pacific via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

(1) W, Lease/Rental of Equipment;
(2) X, Lease/Rental of Facilities;
(3) Y, Construction of Structures and Facilities;
(4) D, Automatic Data Processing and Telecommunications, IT and Telecom-Telecommunications Transmission (D304) and Internet (D322) ONLY;
(5) S, Utilities ONLY;
(6) V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address: https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk at: https://doncmra.nmci.navy.mil.

For the purposes of CMRA reporting, the Federal Supply Code/Product Service Code applicable to the contract is R430.

9.3 *Government Vehicles*. Contractor personnel assigned to operate either Government owned or contractor owned/leased motor vehicles/equipment in performance of this contract shall be certified, by the contractor and at the contractor's expense, as being fully qualified to operate the vehicles/equipment to which they are assigned. The contractor shall document all operator qualification. This documentation shall be provided to the contract administrator prior to an operator engaging in any mode of equipment operation. Documentation shall be retained by the contract administrator. Further, transportation equipment acquired for official purposes by a naval activity and operated by a contractor will be marked to indicate U.S. Government ownership in accordance with the DoD 4500.36-R.